Differential Cryptanalysis can also be applied against stream ciphers, but the implementation might differ by some technical details from the implementation described above.

Література: E. Biham, A. Shamir. Differential Cryptanalysis of DES – like Cryptosystems, Journal of Cryptography. Vol. 1. № 1. pp 3 – 72. 1991. E. Biham, A. Shamir. Differential Cryptanalysis of Data Encryption Standard. Springer – Verlag - 1993. NBS. Data Encryption Standard. U.S. Department of Commitie. FIPS pub.16. January, 1997. E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. Eurocrypt'93. LNCS 765. Springer - 1994.

УДК 621.391

ПРО ВІДНОШЕННЯ ЕКВІВАЛЕНТНОСТІ НА МНОЖИНІ БУЛЬОВИХ ФУНКЦІЙ

Сергій Мельник
Київський військовий інститут управління і зв'язку

Анотація: **Розглядається питання класифікації бульових функцій по відношенню еквівалентності, що визначене на множині F_n всіх бульових функцій від n аргументів, а також деякі криптографічні властивості бульових функцій на одному з визначених класів.**
Summary: **In this article was examined classification of boolean functions on the attitude ecvivalation, which determined on the ensemble F_n of all boolean functions from n arguments, as well as some cryptographs particularity of boolean functions on one of determined classes.**
Ключові слова: **бульова функція, клас, криптографічні властивості.**

Нехай G – деяка група взаємно однозначних перетворень векторного простору Z_n (Z={0,1}). Функції $f_1(x_1,...,x_n)$ та $f_2(x_1,...,x_n)$ називаються еквівалентними відносно групи G, якщо для деякого елемента g∈G

$$f_2(x_1,...,x_n) = f_1(g(x_1,...,x_n)).$$

Представлене відношення є відношенням еквівалентності ([1,2]), за сяким множина всіх бульових функцій розбивається на класи. У випадку, коли $G = \langle S_n, \sum_n \rangle$, класи еквівалентності називають типами, а також якщо $G = S_n$ - розрядами (де S_n - симетрична група перестановок координат векторів із Z_n, $\sum_n$ - група зсувів простору Z_n).

Однотипні функції представляють собою одну логічну форму, записану в різних системах координат, тому значна частина властивостей бульових функцій одного типу співпадає.

З точки зору криптографічних застосувань, важливим є питання про співпадання деяких криптографічних властивостей бульових функцій ([3]), що належать одному типу, а саме: нелінійність, кореляційний імунітет та виконання строгого потокового критерію ("strict avalanche criterion"). З [3] відомо, що перелічені властивості можуть бути сформульовані в термінах перетворення Уолша: $\hat{F}(\overline{w}) = \sum_{\overline{x} \in Z_n} (-1)^{f(\overline{x}) \oplus \overline{wx}}$, де $\overline{xw}$ - скалярний добуток векторів $\overline{x}, \overline{w} \in Z_n$, яке для функцій одного типу відрізняється несуттєво (щодо вказаних властивостей). Отже, для бульових функцій одного типу ці криптографічні властивості співпадають.

Слід відзначити, що в літературі найбільш відомою класифікацією є Гарвардський каталог, що перераховує за типами всі бульові функції від 4-х аргументів і містить інформацію про потужність типів та оптимальну лампову реалізацію функцій – представників типів. Інший, більш точний каталог, був складений групою японських вчених під керівництвом професора Нінномія. Представлений Ніконовим в [2] каталог побудований на використанні принципів класифікації бульових функцій за допомогою графів зв'язності вершин, що декілька полегшує роботу з ним. Каталог Ніконова також містить інформацію про потужність типів та мінімальну структуру реалізації бульових функцій.

Авторами проведений самостійний цикл класифікаційних випробувань. У доповіді представлені деякі результати щодо числа класів та типів при невеликих значеннях n, а також про потужність типів та вказані криптографічні властивості на множині бульових функцій від 3-х аргументів.

Література: 1. Поваров Г. Н. О групповой инвариантности булевых функций. – В сб.: Применение логики в науке и технике. Москва, 1960. 2. Никонов В. Г. Классификация минимальных базисных представлений всех булевых функций от четырех переменных. – В сб.: Обозрение прикладной промышленной математики, серия дискретная математика (1994) 1, выпуск 3. 3. W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions", LNCS 434; Proc. Eurocrypt'89.

УДК 681.511:3

ЧАСТНЫЙ ПОДХОД К ВОПРОСУ ИДЕНТИФИКАЦИИ ПРЕОБРАЗУЮЩЕГО АЛГОРИТМА

Иван Четвериков, Александр Манухин, Светлана Паламарчук
Военный институт Национального технического университета Украины "КПИ"

Анотація: **Частковий підхід до питання ідентифікації перетворюючого алгоритму. Аналіз закритих потоків даних припускає наявність математичної моделі ідентифікації шифратора. Проблема вирішена за допомогою використання спектрального аналізу потоку і побудови профілю потоку.**
Summary: **The private approach to a problem of identification of conversing algorithm. The analysis of the enclosed data-flow guesses presence of the mathematical model of identification of an encoder. The problem is solved by means of a spectrum analysis of a stream and introduction of a profile of a stream enclosed by the relevant algorithm.**
Ключові слова: **захист даних, шаблон, спектральний аналіз.**

I Постановка задачи исследования

Проблема диагностики символьных потоков различных форм (звукового, литерного, изображения) крайне актуальна на различных уровнях управления процессом их обработки. Учитывая направленность деятельности некоторых ведомственных структур, интерес представляет идентификация закрытых потоков {T`}, представляющих собой результат применения криптографических алгоритмов (A):

$$T \to T`, \quad T`= A(T); \qquad \{T`\}_n = \{A(T)\}_n. \tag{1}$$

Закрытый поток данных достаточно просто локализуется методами математической статистики, однако идентификация почерка криптографического алгоритма представляет собой некоторые сложности.

Данная работа посвящена идентификации преобразующего алгоритма (вида специальной аппаратуры), порождающего закрытые потоки {T`} методом их спектрального анализа [2-6].

II Схема информационной обработки потоков данных

Открытая передача закрытых потоков данных по каналам связи осуществляется соответственно функциональной схеме обработки сообщения, тракт прохождения которого представлен на рисунке 1. Он представляет собой набор узлов обработки (1-7), имеющих входные и выходные параметры, а также условия принятия решения. Узлы имеют 1 и 2 входа, 1, 2 и 3 выхода.

Узел № 1 – преобразующий алгоритм источника; узел № 2 – информационный ключ; узел № 3 – стандартизатор потока; узел № 4 – спектральный формирователь; узлы № 5, 7 – спектральные фильтры; узел № 6 – спектральный анализатор. Среду формирования составляют узлы 3, 4; среду исследования – 6 и 7.

Диагностический контур реализован спектральным формирователем объекта исследования, математическим сопроцессором и узлами принятия решения и рассматривается человеко-машинным комплексом "обучение с учителем", обучаемым параметром которого являются характеристика потока.

Работа схемы представляет собой два цикла. Первый цикл осуществляется при нулевых начальных условиях и служит для первичного заполнения спектральных фильтров (условия принятия решения). Цикл № 2 реализует полномасштабную систему анализа и идентификации выбранного потока данных. Рассматриваются раздельно.